PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-122861
(43)Date of publication of application : 28.04.2000

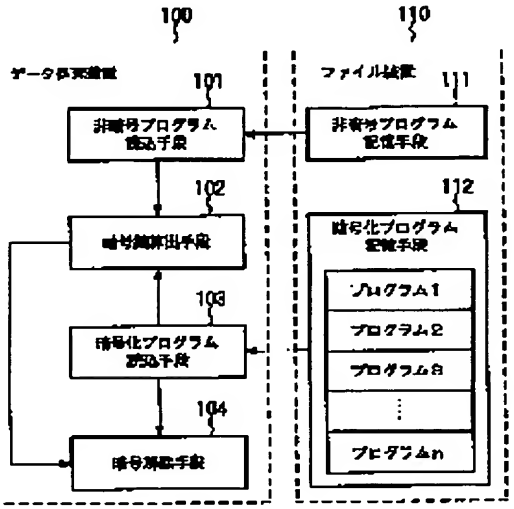
(51)Int.Cl. G06F 9/06
G06F 12/14
G09C 1/00
H04L 9/10
H04L 9/34

(21)Application number : 10-297081
(22)Date of filing : 19.10.1998

(71)Applicant : NEC CORP
(72)Inventor : MORISHITA TAKUYA

(54) ILLEGAL ALTERATION PREVENTION SYSTEM FOR DATA OR THE LIKE AND ENCIPHERING DEVICE USED WITH THE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a technique that prevents an illegal user from altering software and data and illegally attempting to use them.
SOLUTION: An encipher program storing means 112 stores enciphered program codes while being divided into plural blocks. A cryptographic key calculating means 102 uses a one-way function (hash function, etc.), of a program code currently existing on a main storage and calculates a cryptographic key for performing cipher release of an enciphered program code stored in the means 112 to be next executed. When the program code is partially altered to illegally use software, a correct cryptographic key can not be obtained and the execution of the program stops.



LEGAL STATUS

[Date of request for examination] 19.10.1998
[Date of sending the examiner's decision of rejection] 10.04.2001
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－122861
（P2000－122861A）
(43)公開日　平成12年４月28日(2000.4.28)

(51)Int.Cl.'		識別記号	FI			テーマコード'(参考)
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｂ	５Ｂ０１７
	12/14	３２０		12/14	３２０Ｂ	５Ｂ０７６
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｄ	５Ｊ１０４
Ｈ０４Ｌ	9/10		Ｈ０４Ｌ	9/00	６２１Ｚ	
	9/34				６８１	

審査請求　有　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願平10－297081

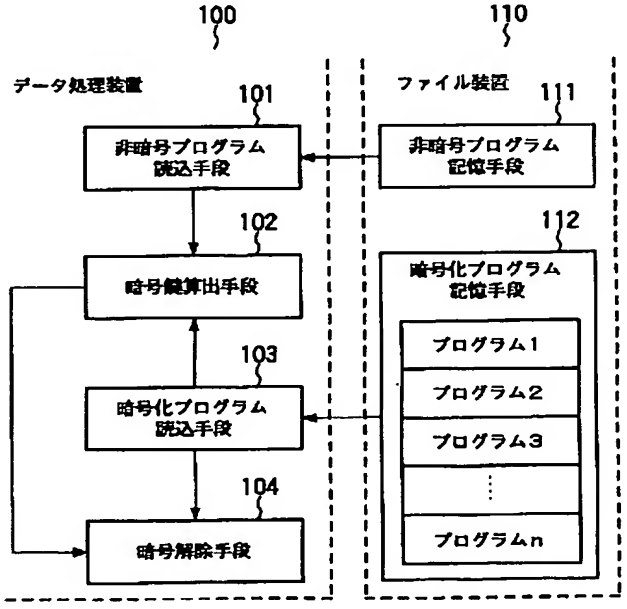
(22)出願日　平成10年10月19日(1998.10.19)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　森下　卓也
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100082935
弁理士　京本　直樹　（外２名）

Ｆターム(参考)　5B017 AA06 AA07 BA07 BB03 CA15
CA16
5B076 AB09 AB10 FA13
5J104 AA12 EA25 NA11 NA12 NA27
NA37 PA14

(54)【発明の名称】　データ等の不正改竄防止システム及びそれと併用される暗号化装置

(57)【要約】
【課題】不正利用者がソフトウェアやデータを改竄し、不正利用する試みを防止できる技術を提供する。
【解決手段】暗号化プログラム記憶手段１１２には暗号化されたプログラムコードが複数のブロックに分割されて格納されている。暗号鍵算出手段１０２は現在主記憶上にあるプログラムコードの一方向関数（ハッシュ関数等）を使用し、暗号化プログラム記憶手段１１２に格納されている次に実行するブロックの暗号化されたプログラムコードを暗号解除するための暗号鍵を算出する。ソフトウェアを不正利用するためにプログラムコードの一部を改竄すると正しい暗号鍵が得られず、プログラムの実行が停止する。



【特許請求の範囲】
【請求項１】データ処理装置とファイル装置とで構成されるデータ等の不正改竄防止システムであり、
前記ファイル装置は、データの先頭ブロックを格納する第１の記憶領域と、この先頭ブロックに後続するｎ個のブロックを格納する第２の記憶領域から構成され、前記ｎ個のブロックの中の１番目のブロックは、前記第１の記憶領域のデータに基づいて生成された第１番目の暗号鍵で暗号化されて格納され、前記ｎ個のブロックの中のｉ（２≦ｉ≦ｎ）番目のブロックは、（ｉ－１）番目のブロックのデータに基づいて生成された第ｉ番目の暗号鍵で暗号化されて格納され、
前記データ処理装置は、
前記第１の記憶領域のデータを読み出す第１の読出手段と、
前記第２の記憶領域のデータを読み出す第２の読出手段と、
前記第２の読出手段により読み出されたｉ番目のブロックを、供給されるｉ番目の暗号鍵を用いて暗号解除する暗号解除手段と、
前記第１の読出手段の出力に基づいて、前記第１番目の暗号鍵を生成し、前記暗号解除手段に供給するとともに、前記暗号解除手段からの（ｉ－１）番目のブロックの暗号解除出力に基づいて、前記第ｉ番目の暗号鍵を生成し、前記暗号解除手段に供給する暗号鍵算出手段とから構成されるデータ等の不正改竄防止システム。
【請求項２】前記データは、プログラムコードであることを特徴とする請求項１に記載のデータ等の不正改竄防止システム。
【請求項３】前記第１の記憶領域には、データの先頭ブロックが前もって定められた第０番目の暗号鍵よって暗号化されて格納されており、前記第１の読出手段は、この第０番目の暗号鍵により前記第１の記憶領域格納データを暗号解除して出力することを特徴とする請求項１、２に記載のデータ等の不正改竄防止システム。
【請求項４】前記暗号鍵算出手段は、１方向関数を用いて、前記第１から第ｎの暗号キーを生成することを特徴とする請求項１、２または３に記載のデータ等の不正改竄防止システム。
【請求項５】データを第１から第（ｎ＋１）番目のブロックに分割する手段と、
前記第１から第ｎ番目のブロックのデータに基づいて、第１から第ｎの暗号鍵を生成する手段と、
前記第１から第ｎの暗号鍵に基づいて前記第２から第（ｎ＋１）番目のブロックをそれぞれ暗号化する暗号化手段と、
前記第１番目のブロックと暗号化された第２から第（ｎ＋１）番目のブロックを出力する出力手段とから構成される暗号化装置。
【請求項６】前記出力手段は、前記第１番目のブロックを前もって定められた第０番目の暗号鍵で暗号化して出力することを特徴とする請求項５に記載の暗号化装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、コンピュータソフトウェアやデータを、不正利用者が改竄し、これらソフトウェアやデータを不正利用（不正コピー等）する試みを防止できる技術に関わる。
【０００２】
【従来の技術】コンピュータソフトウェアの不正コピーを防止するための手法としては、例えば特開平９－２３１１３７「複製判定方法および読出装置」に記載のものが知られている。この従来例では特定の誤り率Ｋを含むキー・コードをＣＤ－ＲＯＭの一部に記録している。この誤り率Ｋは、ＣＤ－ＲＯＭの読み出し装置に設けられている誤り訂正符号化復号化装置では、完全には訂正が不可能な値に定められている。不正にＣＤ－ＲＯＭを複製した場合、このキー・コードの誤り率が変化する。この従来技術では、この現象を利用して、搭載されたＣＤ－ＲＯＭが不正に複製されたＣＤ－ＲＯＭか否かを判定し、複製されたＣＤ－ＲＯＭと判定されたの場合には、読み出し装置が動作しないように構成されている。
【０００３】また、同種の不正コピー防止技術として、特定のキーを持つ簡易なハードウェアをシステムに付加し、プログラムの実行時にこのキーの値が正規の物かを判定して正規の値の場合のみ実行を許可するシステムが広く知られている。
【０００４】
【発明が解決しようとする課題】しかし、これらの従来技術には、次のような問題点があった。
【０００５】第１の問題点は、プログラムコードを解析し、どういった機構で不正コピーを判定しているかを調査することが容易なことである。その理由は、プログラムコードを逆アセンブラツールなどの解析ツールで解析し、その解析結果に基づいて、そのプログラムを改竄することにより、不正利用が可能となるためである。
【０００６】第２の問題点は、プログラムコードを改竄されるとコピー媒体での実行を防げることができないことである。その理由は、コピー媒体の判定を行っている部分のプログラムコードを、コピーされた媒体を検出しても、常にオリジナルな媒体と判定するように改竄された場合、コピー媒体でそのソフトウェアを実行されることを防ぐことはできないためである。同様の問題は、プログラムに限らず、一般のデータでも起こりうる。
【０００７】
【課題を解決するための手段】本発明のデータ等の不正改竄防止システムは、データ処理装置とファイル装置とで構成されるデータ等の不正改竄防止システムであり、前記ファイル装置は、データの先頭ブロックを格納する第１の記憶領域と、この先頭ブロックに後続するｎ個の

ブロックを格納する第２の記憶領域から構成され、前記ｎ個のブロックの中の１番目のブロックは、前記第１の記憶領域のデータに基づいて生成された第１番目の暗号鍵で暗号化されて格納され、前記ｎ個のブロックの中のｉ（２≦ｉ≦ｎ）番目のブロックは、（ｉ－１）番目のブロックのデータに基づいて生成された第ｉ番目の暗化鍵で暗号化されて格納され、前記データ処理装置は、前記第１の記憶領域のデータを読み出す第１の読出手段と；前記第２の記憶領域のデータを読み出す第２の読出手段と；前記第２の読出手段により読み出されたｉ番目のブロックを、供給されるｉ番目の暗号鍵を用いて暗号解除する暗号解除手段と；前記第１の読出手段の出力に基づいて、前記第１番目の暗号鍵を生成し、前記暗号解除手段に供給するとともに、前記暗号解除手段からの（ｉ－１）番目のブロックの暗号解除出力に基づいて、前記第ｉ番目の暗号鍵を生成し、前記暗号解除手段に供給する暗号鍵算出手段；とから構成される。

【０００８】また、本発明の暗号化装置は、データを第１から第（ｎ＋１）番目のブロックに分割する手段と；第１から第ｎ番目のブロックのデータに基づいて、第１から第ｎの暗号鍵を生成する手段と；前記第１から第ｎの暗号鍵に基づいて前記第２から第（ｎ＋１）番目のブロックをそれぞれ暗号化する暗号化手段と；前記第１番目のブロックと暗号化された第２から第（ｎ＋１）番目のブロックを出力する出力手段；とから構成される。

【０００９】

【発明の実施の形態】図１を参照すると、本発明のソフトウェアの不正利用防止システムの一実施形態は、プログラム制御により動作するデータ処理装置１００と、ファイル装置１１０とから構成されている。データ処理装置１００は、非暗号プログラム読込手段１０１と、暗号鍵算出手段１０２と、暗号化プログラム読込手段１０３と、暗号解除手段１０４を含む。ファイル装置１１０は、非暗号プログラム記憶手段１１１と暗号化プログラム記憶手段１１２を含む。

【００１０】これらの手段はそれぞれ概略つぎのように動作する。

【００１１】非暗号プログラム記憶手段１１１には暗号化されていないプログラムコードが格納されている。暗号化プログラム記憶手段１１２には暗号化されたプログラムコードが複数のブロック１、２、・・・ｎに分割されて格納されている。これらは、非暗号プログラム記憶手段１１１に格納された暗号化されていないプログラムコード、暗号化されたブロック１、２、・・・ｎの順に、データ処理装置１００に読み込まれるものとする。

【００１２】非暗号プログラム読込手段１０１は、非暗号プログラム記憶手段１１１から、図示していない主記憶上に、暗号化されていないプログラムコードを読み込む。

【００１３】暗号鍵算出手段１０２は、この主記憶上にあるプログラムコードの一方向関数（ハッシュ関数など）を使用して、読み込まれる暗号化されたプログラムコードブロックを平文化するための暗号鍵を生成する。暗号化プログラム読込手段１０３は、暗号化プログラム記憶手段１１２から主記憶上に次に実行する暗号化されたプログラムコードを読み込む。暗号解除手段１０４は、暗号鍵算出手段１０２が算出した暗号鍵を使用して、暗号化されたプログラムコードの暗号を解除する。

【００１４】まず、図４を参照して、ファイル装置１１０に書き込まれるデータを作成する暗号化装置につき、説明する。図４は、ファイル装置１１０に書き込まれるデータを作成するための暗号化装置の構成を示すブロック図である。

【００１５】ファイル装置に格納されるべき、プログラムコードは、分岐回路２０１に供給される。分岐回路は、供給されたプログラムコードを、（ｎ＋１）個のブロックに分割し、最初のブロックを図１の非暗号プログラム記憶手段１１１に書き込むとともに、暗号鍵算出手段１０２に供給する。また分岐回路は、最初のブロックを出力後、最初のブロック（第０番目のブロック）を除くｎ個のブロックを順に、遅延回路２０３及び暗号鍵算出手段１０２に出力する。

【００１６】暗号鍵算出手段は、分岐回路２０１から最初のブロックが供給されると、この最初のブロックのプログラムコードからハッシュ関数等の一方向関数を用いて、最初のブロックの次のブロック（第１番目のブロック）のデータを暗号化するための第１の暗号鍵を算出する。この第１の暗号鍵の出力が終了すると、この暗号鍵算出手段１０２には、第１番目のブロック、第２番目のブロック、・・・第ｎ番目のブロックが順次供給され、同様にして、第２の暗号鍵、・・・第ｎの暗号鍵が、順次出力され暗号化器２０４に供給される。

【００１７】一方、遅延回路２０３は、分岐回路から順次供給される第１番目から第ｎ番目のブロックは、遅延回路に２０３により、１ブロック分遅延されて暗号化器に供給される。この結果、第１のブロックは、第０のブロックのデータにより生成された第１の暗号鍵により暗号化され、図１の暗号化プログラム記憶手段１１２に格納される。第２のブロックは、第１のブロックのデータにより生成された第２の暗号鍵により暗号化され、図１の暗号化プログラム記憶手段１１２に格納される。以下同様にして、第ｉ番目のブロックは、第（ｉ－１）番目のブロックのデータにより生成された第ｉの暗号鍵により暗号化され、図１の暗号化プログラム記憶手段１１２に格納される。

【００１８】このようにして、図１の非暗号プログラム記憶手段１１１には暗号化されていないプログラムコードが格納され、暗号化プログラム記憶手段１１２には暗号化されたプログラムコードが複数のブロック１、２、・・・ｎに分割されて格納される。

【００１９】次に、図２のフローチャートを参照して本実施形態の全体の動作について詳細に説明する。

【００２０】暗号化プログラム記憶手段１１２には、非暗号化プログラム記憶手段１１１内に格納されたプログラムコードに後続するプログラムコードが複数のブロックに分割されて格納されている。暗号化プログラム記憶手段１１２には、それぞれのブロックのプログラムコードは、一つ前のブロックのプログラムコードのハッシュ値を暗号鍵に使用して暗号化され、格納されている。

【００２１】まず、ステップＡ１では、非暗号プログラム読込手段１０１は、非暗号プログラム記憶手段１１１から暗号されていないプログラムコードを主記憶上に読み込み、プログラムコードの実行を開始する。この処理は通常、オペレーティングシステムのプログラム実行機構で管理されている。

【００２２】次に、ステップＡ２では、暗号鍵算出手段１０２は、非暗号プログラム読込手段１０１が主記憶上に読み込んだプログラムコードをハッシュ関数などの一方向関数で変換し、暗号鍵を生成する。

【００２３】ステップＡ３では、暗号化プログラム読込手段１０３は、暗号化プログラム記憶手段１１２から主記憶上に次に実行する暗号化されたプログラムコードを読み込む。

【００２４】ステップＡ４では、暗号解除手段１０４は、暗号鍵算出手段１０２が算出した暗号鍵を使用して、暗号化されたプログラムコードの暗号を解除する。

【００２５】ステップＡ５では、暗号鍵算出手段１０２は、暗号解除されたプログラムコードのハッシュ値を算出し、これを次回の暗号解除時の暗号鍵とする。

【００２６】次に、ステップＡ６では、現在主記憶上にある暗号解除されたプログラムコードを実行する。この処理の中で、不正コピーの判定等を行う。

【００２７】ステップＡ７では、暗号化プログラム記憶手段１１２内の全てのブロックのプログラムコードにつき、ステップＡ３からＡ６までの処理が行われたか否かが判定され、全てのブロックのプログラムコードについて処理が実行されていない場合には、データ処理装置の動作は、ステップＡ３に戻る。

【００２８】図３は不正利用者によるプログラムコードの改竄の試みが行われなかった場合の動作を現す説明図である。プログラムコードの改竄が行われなかった場合には、暗号化されたプログラムコードを暗号解除するための暗号鍵ａ，ｂ，ｃは正しい値が得られる。

【００２９】非暗号化プログラム記憶手段１１１に格納されている暗号化されていないプログラムコード１を改竄した場合、ステップＡ２で算出される暗号鍵は、本来の暗号鍵ａと全く異なった物となる。このため、ステップＡ４で暗号解除されたプログラムコード２は本来のプログラムコードと全く異なったコードとなり、以降のプログラムは正常に動作しなくなる。暗号化プログラム記憶手段１１２内のプログラムコードが改竄された場合にも、改竄されたブロックより後のブロックのプログラムコードは、ステップＡ４で暗号解除されても、本来のプログラムコードと全く異なったコードとなり、以降のプログラムは正常に動作しなくなる。

【００３０】このようにプログラムコードを一個所改竄すると、以降のプログラムを正常に動作させるためには、全てのブロックの暗号鍵を何らかの手段で取得し、暗号解除手段１０４が使用する暗号鍵として使用するように改竄する必要がある。このような不正利用者にとって好ましい改竄は、ブロックの数を増やすほど困難になる。

【００３１】この実施形態では、改竄検出の対象をプログラムコードとしたが、暗号鍵の生成時にデータ領域の一方向関数を使用することによって、データの改竄を検出することも可能である。この場合には、上述の説明において、「プログラム」を、「データ」と読み替えれば良い。

【００３２】また、以上説明した実施形態では、非暗号プログラム記憶手段１１１内のプログラムコードあるいはデータは、暗号化されずに平文にままで格納されているものとして説明していたが、この非暗号プログラム記憶手段１１１内のプログラムコードあるいはデータは、前もって定められた暗号鍵により、暗号化されていても良いことは明かであろう。この場合には、図１の非暗号プログラム読み込み手段１０１は、この前もって定められた暗号鍵に基づいて、記憶手段１１１内のデータを暗号解除して出力する機能を併せて有する。

【００３３】

【発明の効果】本発明では、プログラムコードの大部分が暗号化されているため、逆アセンブラツールなどの解析ツールでプログラムコードを解析すること自体が困難である。また、本発明では、暗号鍵算出手段１０２が現在実行しているプログラムコードの一方向関数を暗号解除鍵として算出し、次に実行するプログラムコードの暗号化解除に使用しているため、プログラムコードを改竄して不正利用することが困難である。

【図面の簡単な説明】

【図１】本発明の一実施形態を示すブロック図である。

【図２】本発明の一実施形態の動作を説明するためのフローチャートである。

【図３】不正利用者によるプログラムコードの改竄の試みが行われなかった場合の動作を現す説明図である。

【図４】本発明のファイル装置に書き込まれるデータを作成するための暗号化装置の構成を示すブロック図である。

【符号の説明】

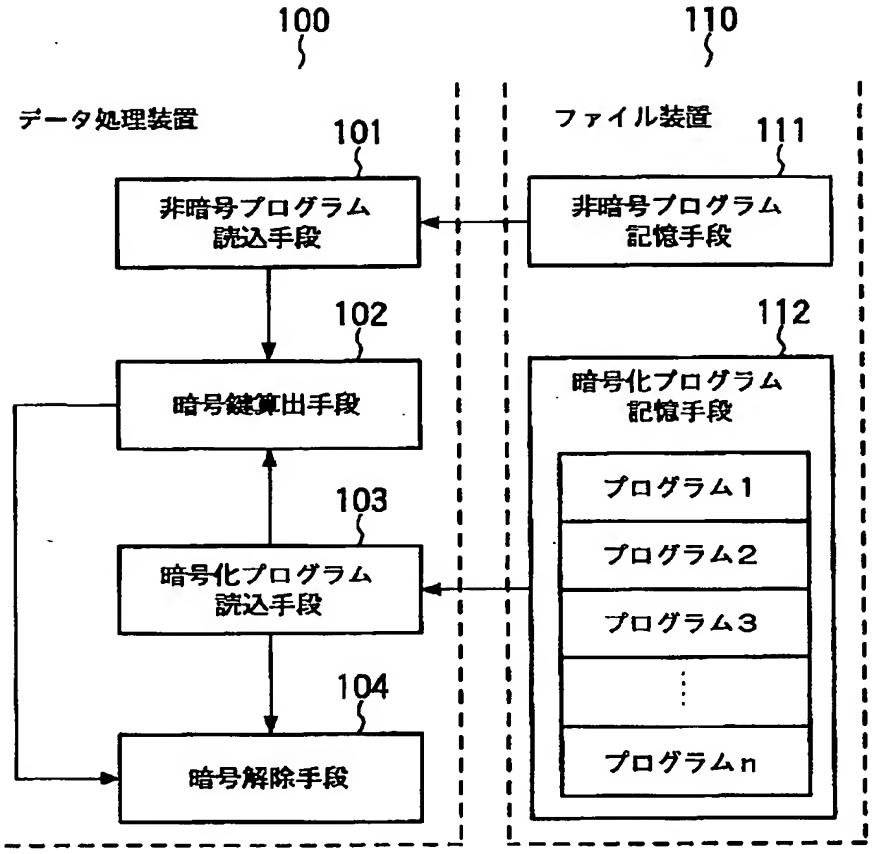
１００　データ処理装置

１０１　非暗号プログラム読込手段

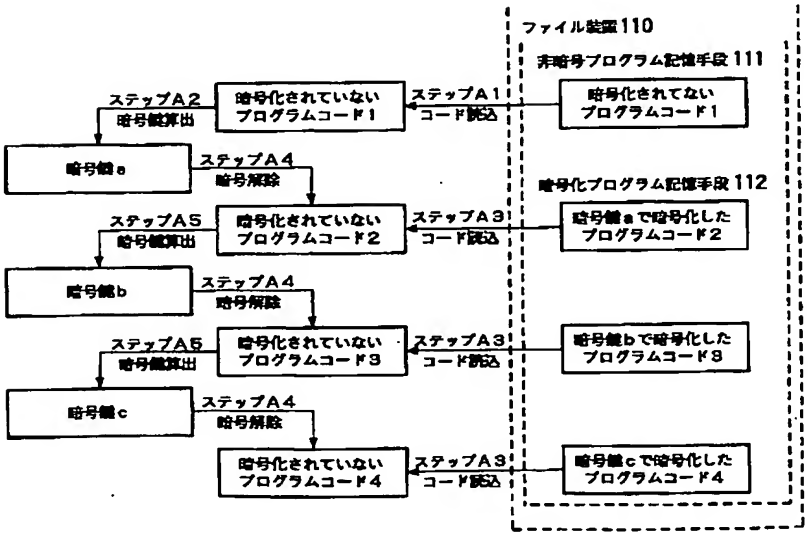
１０２　暗号鍵算出手段

１０３　暗号化プログラム読込手段
１０４　暗号解除手段
１１０　ファイル装置
１１１　非暗号プログラム記憶手段
１１２　暗号化プログラム記憶手段
２０１　分岐回路
２０３　遅延回路
２０４　暗号化器

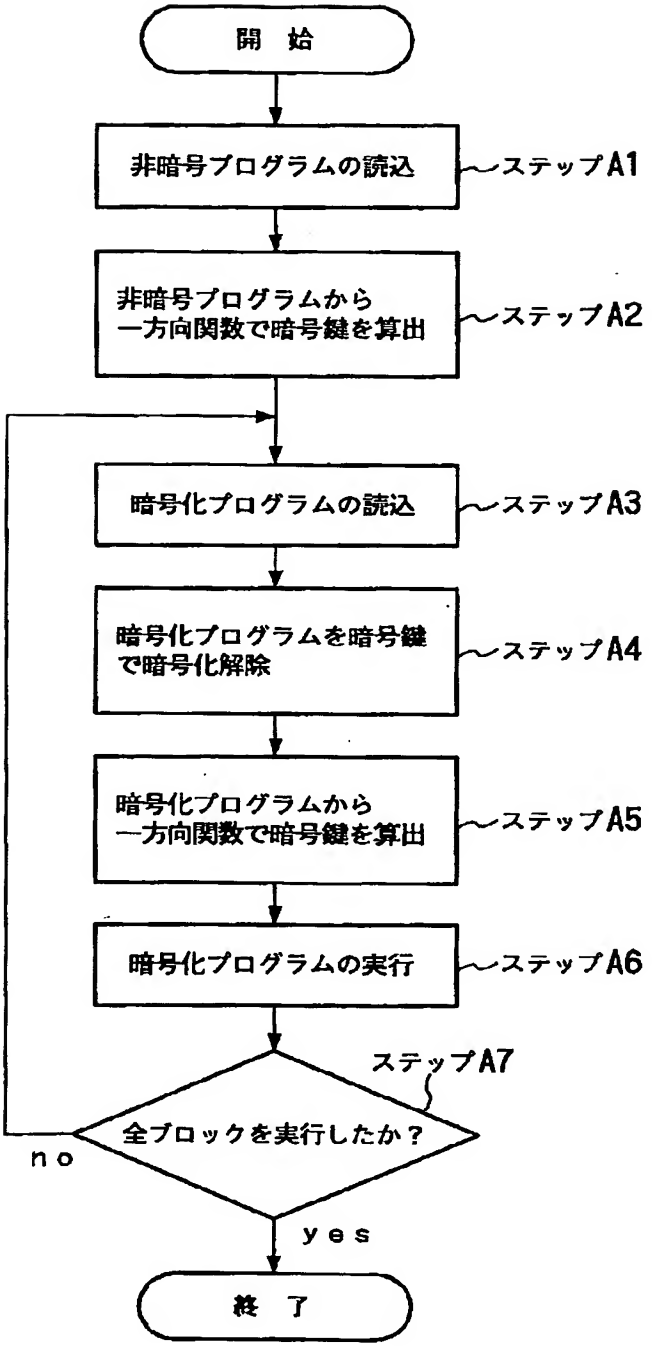
【図１】



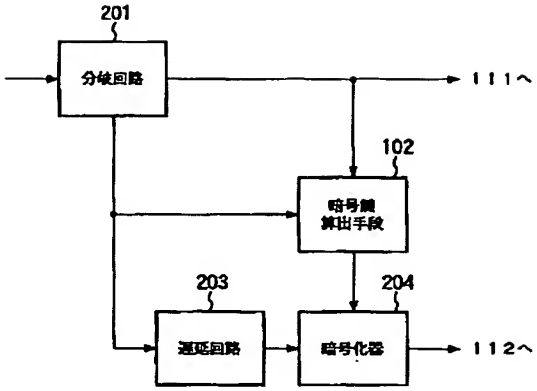
【図３】



【図２】


開　始
非暗号プログラムの読込
ステップA1
非暗号プログラムから
一方向関数で暗号鍵を算出
ステップA2
暗号化プログラムの読込
ステップA3
暗号化プログラムを暗号鍵
で暗号化解除
ステップA4
暗号化プログラムから
一方向関数で暗号鍵を算出
ステップA5
暗号化プログラムの実行
ステップA6
ステップA7
全ブロックを実行したか？
no
yes
終　了

【図４】


201
分岐回路
111へ
102
暗号鍵
算出手段
203
204
遅延回路
暗号化器
112へ